

# PATENT ABSTRACTS OF JAPAN

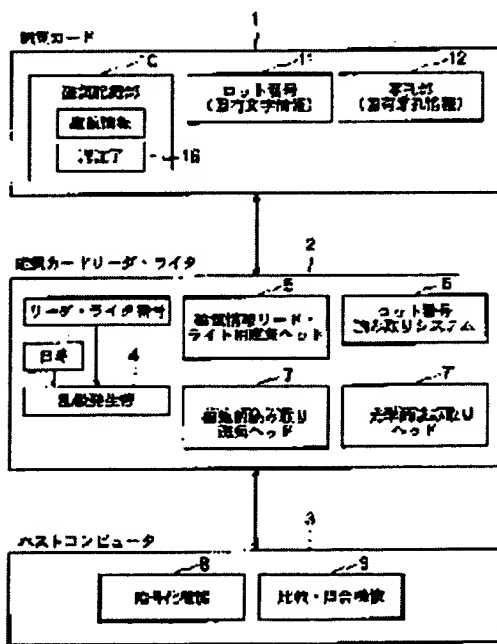
(11)Publication number : 10-247229

(43)Date of publication of application : 14.09.1998

(51)Int.Cl. G06K 17/00  
G11B 5/02

(21)Application number : 09-049217 (71)Applicant : TOKIN CORP  
(22)Date of filing : 04.03.1997 (72)Inventor : INABE TOSHIHISA

## (54) MAGNETIC CARD SYSTEM



### (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent forgery by comparing and collating an authenticater within a host computer prepared by a ciphering function obtained by ciphering frequency information and card characteristic information with card characteristic perforated information as a key and an authenticater within the magnetic card read into in advance.

**SOLUTION:** At the time of authenticating a card, the authenticater within the magnetic card 16 recorded on the magnetic card 1 is read by a magnetic head for reading and writing magnetic information. Next, characteristic perforated information obtained by reading a perforated part 12 by means of an optically reading head 7' and characteristic perforated information obtained by reading the perforated part 12 by means of a

magnetically reading head 7 are compared and collated with each other within the host computer 3 to confirm the authenticity of characteristic perforated information. If being correct, an authenticater is prepared within the host computer 3 by setting frequency information read by the head 5, a lot number 11 read by a lot number reading system 6 and characteristic perforated information 12 read by the head 7' to be keys to compare and collate with the authenticater within the magnetic card 16 read in advance.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-247229

(43)公開日 平成10年(1998) 9月14日

(51)Int.Cl.<sup>8</sup>

識別記号

F I

G 0 6 K 17/00

G 0 6 K 17/00

T

G 1 1 B 5/02

G 1 1 B 5/02

A

Z

審査請求 未請求 請求項の数 6 O L (全 7 頁)

(21)出願番号 特願平9-49217

(22)出願日 平成9年(1997) 3月4日

(71)出願人 000134257

株式会社トーキン

宮城県仙台市太白区郡山6丁目7番1号

(72)発明者 稲部 敏久

宮城県仙台市太白区郡山6丁目7番1号

株式会社トーキン内

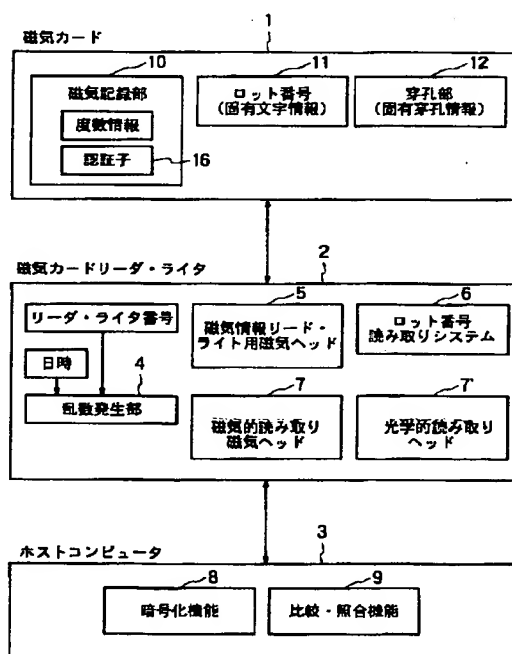
(74)代理人 弁理士 後藤 洋介 (外2名)

(54)【発明の名称】 磁気カードシステム

(57)【要約】

【課題】 予め記憶されたID情報、金銭価値が複製されて次々と偽造されることのない磁気カードを提供することである。

【解決手段】 磁気カード1、磁気カードリーダー・ライター2及びホストコンピュータ3から構成されている。磁気カードリーダー・ライター2には、リーダー・ライター番号及び日時を種として乱数を作成する乱数発生部4、磁気情報リード・ライト用磁気ヘッド5、磁気カード1が具備する固有文字情報であるロット番号11の読取りシステム6及び磁気カード1が具備する固有穿孔情報である穿孔部12の磁気的読取り用磁気ヘッド7及び光学的読取りヘッド7'が、ホストコンピュータ3には、暗号化機能8及び認証子比較・照合機能9が設けられている。



## 【特許請求の範囲】

【請求項1】 磁気カード、磁気カードリーダー・ライター、該磁気カードリーダー・ライターとオンラインで接続されているホストコンピュータからなる磁気カードシステムにおいて、前記磁気カードは、磁気による度数情報、文字によるカード固有文字情報、穿孔によるカード固有穿孔情報、前記度数情報及び前記カード固有文字情報、及び前記カード固有穿孔情報を鍵として暗号化した認証子を具備し、前記磁気カードリーダー・ライターは、リーダー・ライト磁気ヘッド、前記カード固有文字情報を読取る文字情報の読取り手段、前記カード固有穿孔情報を読取る穿孔情報読取り手段、乱数発生部、穿孔機能を具備し、更に、前記ホストコンピュータは、前記度数情報及び前記カード固有文字情報を前記カード固有穿孔情報を鍵として暗号化する暗号化機能、該暗号化機能により作成されたホストコンピュータ内認証子と先に読込んだ磁気カード内認証子とを比較、照合する認証子照合機能を具備することを特徴とする磁気カードシステム。

【請求項2】 前記穿孔情報読取り手段は光学的及び磁氣的に読み取ることを特徴とする請求項1記載の磁気カードシステム。

【請求項3】 予めカード内に記録されている前記ホストコンピュータ内認証子と前記ホストコンピュータ内で前記度数情報及びカード固有文字情報を前記カード固有穿孔情報を鍵として暗号化した前記ホストコンピュータ内認証子とを比較照合することにより前記磁気カード内認証子の正当性を確認することを特徴とする請求項1記載の磁気カードシステム。

【請求項4】 前記カード固有穿孔情報は、前記磁気カードリーダー・ライター内に具備する乱数発生部により生成する乱数と1:1に対応するコード情報に変換し、該コード情報に基づいて穿孔して設けることを特徴とする請求項1又は2記載の磁気カードシステム。

【請求項5】 前記磁気カードは使用する毎に穿孔され、その穿孔数は使用前の穿孔数と同数以上であることを特徴とする請求項1乃至3のいずれか一つに記載の磁気カードシステム。

【請求項6】 前記カード固有穿孔情報を光学的に検知すると共に、前記カード固有穿孔情報を磁氣的に検知することによって得られる両カード固有穿孔情報とを比較照合することにより前記カード固有穿孔情報の正当性を確認することを特徴とする請求項1記載の磁気カードシステム。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、偽造・変造がしにくく、セキュリティ性に富む磁気カードシステムに関するものである。

【0002】

【従来の技術】一般に、カードの磁気記録層に予め金銭

価値が記憶され、取引時に売買代金が減額されるように構成された、所謂、前払い式プリペイドカードとして利用される磁気カードが知られている。このような磁気カードは、鉄道代金の支払い、レジャー施設利用料の支払い、また、商店街での商品購入代金の支払い等に広く利用されている。

【0003】

【発明が解決しようとする課題】これら磁気カードの安全性は、磁気記録層に記憶された、例えば、ID情報等を照合する方法で確保するのが一般的であるが、それだけでは磁気記録層の直接書き換え、あるいは、磁気カードと磁気カードリーダー・ライター間の通信路への割り込みによる改竄等の不正行為への対策としては不十分であった。即ち、前記のような磁気カードは、予め金銭価値が磁気記録層に記録されてから利用者に手渡されるため、悪用者が元磁気カードのID情報、金銭価値データを別の磁気カードに複製し、次々と新たな磁気カードを偽造するというおそれがあった。

【0004】本発明の目的は、予め記憶されたID情報、金銭価値が複製されて次々と偽造されることのない磁気カードを提供することである。

【0005】

【課題を解決するための手段】本発明によれば、磁気カード、磁気カードリーダー・ライター、該磁気カードリーダー・ライターとオンラインで接続されているホストコンピュータからなる磁気カードシステムにおいて、前記磁気カードは、磁気による度数情報、文字によるカード固有文字情報、穿孔によるカード固有穿孔情報、前記度数情報及び前記カード固有文字情報、及び前記カード固有穿孔情報を鍵として暗号化した認証子を具備し、前記磁気カードリーダー・ライターは、リーダー・ライト磁気ヘッド、前記カード固有文字情報を読取る文字情報の読取り手段、前記カード固有穿孔情報を読取る穿孔情報読取り手段、乱数発生部、穿孔機能を具備し、更に、前記ホストコンピュータは、前記度数情報及び前記カード固有文字情報を前記カード固有穿孔情報を鍵として暗号化する暗号化機能、該暗号化機能により作成されたホストコンピュータ内認証子と先に読込んだ磁気カード内認証子とを比較、照合する認証子照合機能を具備することを特徴とする磁気カードシステムが得られる。

【0006】さらに、本発明によれば、前記穿孔情報読取り手段は光学的及び磁氣的に読み取ることを特徴とする磁気カードシステムが得られる。

【0007】さらに、本発明によれば、予めカード内に記録されている前記ホストコンピュータ内認証子と前記ホストコンピュータ内で前記度数情報及びカード固有文字情報を前記カード固有穿孔情報を鍵として暗号化した前記ホストコンピュータ内認証子とを比較照合することにより前記磁気カード内認証子の正当性を確認することを特徴とする磁気カードシステムが得られる。

【0008】さらに、本発明によれば、前記カード固有穿孔情報は、前記磁気カードリーダー・ライタ内に具備する乱数発生部により生成する乱数と1:1に対応するコード情報に変換し、該コード情報に基づいて穿孔して設けることを特徴とする磁気カードシステムが得られる。

【0009】さらに、本発明によれば、前記磁気カードは使用する毎に穿孔され、その穿孔数は使用前の穿孔数と同数以上であることを特徴とする磁気カードシステムが得られる。

【0010】さらに、本発明によれば、前記カード固有穿孔情報を光学的に検知すると共に、前記カード固有穿孔情報を磁気的に検知することによって得られる両カード固有穿孔情報とを比較照合することにより前記カード固有穿孔情報の正当性を確認することを特徴とする磁気カードシステムが得られる。

【0011】

【作用】カード固有文字情報は、例えば、ロット番号に代表される情報で、磁気カード製造時に大雑把に磁気カードの素性を決定可能である。

【0012】カード固有穿孔情報は、例えば、カードリーダー・ライタ内のリーダー・ライタ番号、日時等を種として発生する乱数に1:1に対応して穴開け位置を変化させることにより無作為に決定することが可能である。

【0013】従って、カード固有文字情報及びカード固有穿孔情報の組合せにより磁気カード毎に特定の固有情報を無作為に選択することができる。

【0014】カード発行は、前記磁気カードへの前記ホストコンピュータからの指示による度数情報の磁気的書込み、前記リーダー・ライタで発生させた乱数に1:1に対応する穿孔からなる前記カード固有穿孔情報を前記磁気カードへ施し、更に、前記度数情報及び前記カード固有文字情報を前記カード固有穿孔情報を鍵として前記ホストコンピュータ上で暗号化した磁気カード内認証子の前記磁気カードへの磁気的書込みにより行なう。

【0015】一方、カード認証は、前記磁気カードより読み込まれた前記度数情報及び前記カード固有文字情報を前記カード固有穿孔情報を鍵としてホストコンピュータ内で暗号化したホストコンピュータ内認証子と予め前記磁気カードに記録されている磁気カード内認証子とを比較照合することにより正当性を確認する。

【0016】この時、前記カード固有穿孔情報を光学的に検知することによって得られるカード固有穿孔情報と前記カード固有穿孔情報を磁気的に検知することによって得られるカード固有穿孔情報とを比較照合することによって、前記カード固有穿孔情報の正当性（例えば、穴埋め等による不正）を確認すればより効果的である。

【0017】即ち、前記カード固有穿孔情報を穴埋め等により改竄しようとしても、光学的な穴位置情報と磁気ヘッドによるスキャン再生出力情報が一致しなければ偽造・変造品と判断可能である。

【0018】従って、磁気情報であるカード固有文字情報、度数情報、及び磁気カード内認証子を偽造・変造の目的で書き換えたとしても、物理的に偽造の困難なカード固有穿孔情報を鍵として暗号化するため、磁気情報の矛盾を検出することが可能である。

【0019】更に、前記度数情報、前記カード固有穿孔情報、磁気カード内認証子は、磁気カード使用の度に、毎回変わるため偽造されにくい。

【0020】また、たとえ磁気カードリーダー・ライタを盗難されたとしても、前記リーダー・ライタには、乱数発生部のみが搭載され、暗号化機能、認証子照合機能は搭載されていないためセキュリティは安全である。

【0021】

【発明の実施の形態】以下、本発明の一実施の形態について図面を参照して説明する。図1は、本発明の一実施の形態の磁気カードシステムのブロック図を示す。システムは、磁気カード1、磁気カードリーダー・ライタ2及びホストコンピュータ3から構成されている。磁気カードリーダー・ライタ2には、リーダー・ライタ番号及び日時を種として乱数を作成する乱数発生部4、磁気情報リード・ライト用磁気ヘッド5、磁気カード1が具備する固有文字情報であるロット番号11の読取りシステム6及び磁気カード1が具備する固有穿孔情報である穿孔部12の磁気的読取り用磁気ヘッド7及び光学的読取りヘッド7'が、ホストコンピュータ3には、暗号化機能8及び認証子比較・照合機能9が設けられている。

【0022】図2は、本発明の一実施の形態の磁気カードの概略図を示し、JIS X6311（プリペイドカード－買物用カード－物理的特性及び形状・寸法）、JIS X6313（プリペイドカード－買物用カード－磁気的特性及び情報記録様式）、JIS X6314（プリペイドカード－買物用カード－磁気記録フォーマット）に準拠して作成されている。磁気カードの磁気記録部10、固有文字情報として8文字からなるロット番号11、固有穿孔情報を記録する穿孔部12を設けている。磁気記録部10には、度数情報及び認証子が記録されている。穿孔部12は、光学的には、4行×64列、磁気的には4トラック×64ビット、即ち、256個に論理的に分割されている。

【0023】カード発行時には、ホストコンピュータ3からのコマンドで度数情報を磁気ヘッド5で書込む。次に、磁気カードリーダー・ライタ2内でリーダー・ライタ番号及び日時から作成した乱数をコード化して固有穿孔情報とし、磁気カード1上の穿孔部12のマトリックス上の3個所に穿孔を施す（この3個所の組合せは、2、76×10°通りである）。更に、度数情報及びカード上に印刷されたロット番号11を穿孔部12上の固有穿孔情報を鍵として暗号化を行い、認証子16を磁気ヘッド5で書込む。

【0024】カード認証時には、磁気カード1上に記録

されている磁気カード内認証子16を磁気情報リード・ライト用磁気ヘッド5で読込む。次に、穿孔部12を光学的読取りヘッド7'で走査して読み込んだ固有穿孔情報と穿孔部12を磁氣的読取りヘッド7で走査して読み込んだ固有穿孔情報をホストコンピュータ3内で比較・照合して固有穿孔情報の正当性を確認する。もし正しければ、磁気カード1より磁気情報リード・ライト用磁気ヘッド5で読込まれた度数情報及びロット番号読取りシステム6で読込まれたロット番号11を、穿孔部12を光学的読取りヘッド7'で走査して読み込んで得た固有穿孔情報12を鍵としてホストコンピュータ3内で暗号化してホストコンピュータ内認証子17を作成し、先に読込んだ磁気カード内認証子16と比較・照合を行なう。

【0025】カード返却時には、穿孔数を1個とする以外は、前記カード発行時と同様な操作を行なって、磁気カード1内へ変更情報を記録する。

【0026】以上の流れを要約すると、図3（カード発行、カード返却）及び図4（カード認証）のようになる。

【0027】

【発明の効果】以上説明したように、本発明によれば、予め記憶されたID情報、金銭価値が複製されて次々と偽造されることのない磁気カードを提供することができ\*

＊る。

【図面の簡単な説明】

【図1】本発明による磁気カードシステムの一実施の形態を示すブロック図である。

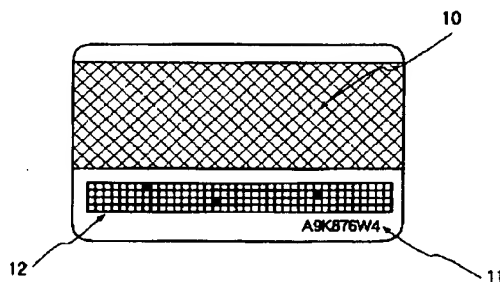
【図2】本発明による磁気カードの一実施の形態における平面図である。

【図3】本発明による磁気カードシステムの一実施の形態におけるカード発行流れ図である。

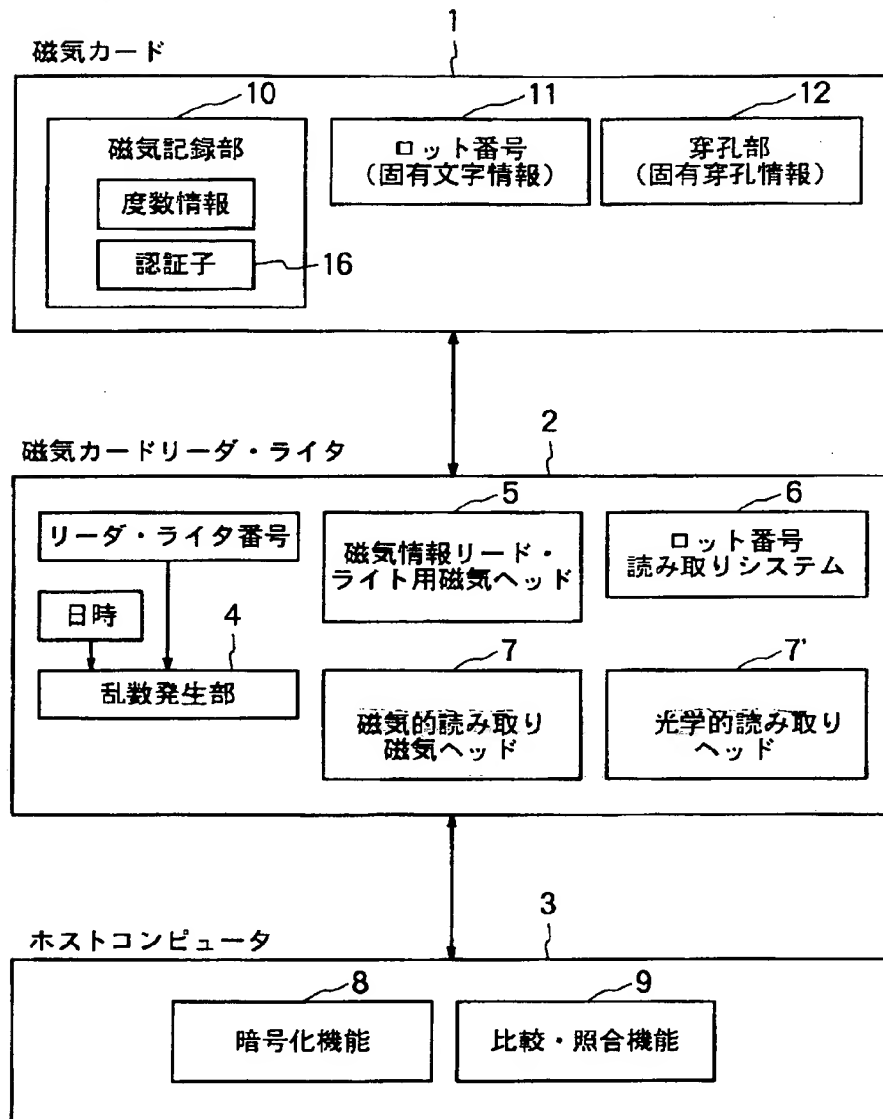
【図4】本発明による磁気カードシステムの一実施の形態におけるカード認証流れ図である。

- 1 磁気カード
- 2 磁気カードリーダー・ライター
- 3 ホストコンピュータ
- 4 乱数発生部
- 5 磁気情報リード・ライト用磁気ヘッド
- 6 ロット番号読取りシステム
- 7 磁氣的読取りヘッド
- 7' 光学的読取りヘッド
- 8 暗号化機能
- 9 比較・照合機能
- 10 磁気記録部
- 11 ロット番号
- 12 穿孔部

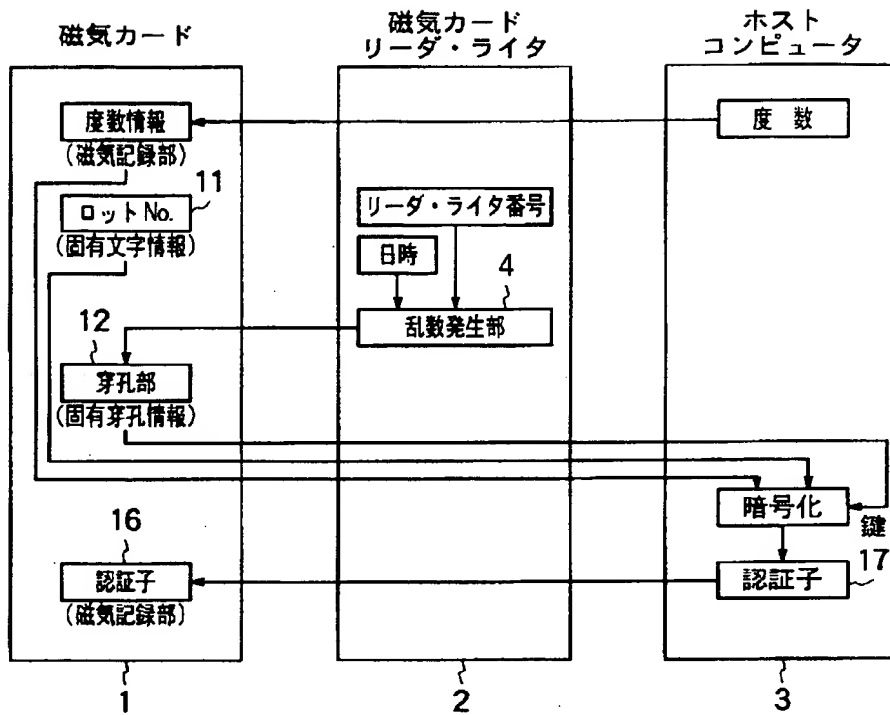
【図2】



【図1】



【図3】



【図4】

